

IN THE CLAIMS

Please amend the claims as shown below. Please cancel Claims 2 and 5 without prejudice. This listing of claims will replace all prior versions and listings of claims in the Application.

1. (Currently Amended) A method for preventing unauthorized transfer of data between a portable computer system and systems of data storage and communication including an other computer, said method comprising ~~the steps of:~~
  - a) automatically receiving identification authentication information for said portable computer  
system by transferring identification authentication information between a portable computer system and a communication interface device, wherein said authentication information comprises a unique identity for said portable computer wherein said portable computer comprises a palmtop computer and said interface device comprises a palmtop computer system cradle;
  - b) comparing said identification authentication information with a list of authorized portable computer system identities;
  - c) determining whether said portable computer system identity is authorized based on said identification authentication information and said unique identity;
  - d) enabling communication between said portable computer system and said other computer provided said identity is authorized and disabling said communication if said identity is not authorized; and
  - e.) enabling decryption of encrypted data from said portable computer system provided said identity is authorized and disabling decryption if said identity is not authorized.
2. (Cancelled)

3. (Original) The method as recited in Claim 2 wherein said information is transferred from said portable device to said interface device to uniquely identify said portable device to said interface device.

4. (Original) The method as recited in Claim 2 wherein said information is transferred from said interface device to said portable device to uniquely identify said interface device to said portable device.

5. (Cancelled)

6. (Currently Amended) The method as recited in Claim 1 wherein said step b) comprises ~~the steps of:~~:

recognizing said identification authentication information as an indication of unique identity of the source sending said information; and indexing said unique identity to a list of programmed identities.

7. (Currently Amended) The method as recited in Claim 1 wherein said step c) comprises ~~the steps of:~~:

reacting to positive indexing match as an authenticated authorized identity and to negative indexing match as an unauthorized identity; and authorizing communications enablement in response to an authenticated authorized identity, and prohibiting communications in response to an unauthorized identity.

8. (Currently Amended) The method as recited in Claim 1 wherein said step d) comprises: ~~the steps of allowing said portable computer to synchronize with said other computer upon authorization of communication and preventing synchronization upon prohibition of communication.~~

allowing said portable computer to synchronize with said other computer upon authorization of communication; and  
preventing synchronization upon prohibition of communication.

9. (Currently Amended) The method as recited in Claim 1 wherein said step e) comprises ~~the steps of disclosing a specific key value with which said data is encrypted upon authorization of communication and not disclosing said specific key value upon prohibition of communication.~~

disclosing a specific key value with which said data is encrypted upon authorization of communication; and  
not disclosing said specific key value upon prohibition of communication.

10. (Currently Amended) A system for preventing unauthorized transfer of data between a portable computer system and a host system, comprising:

- a) a portable computer device capable of synchronizing with said host;
- b) an interface device compatible to receive said portable computer device and coupled with said host system and capable of facilitating communication between said portable computer device and said host system;
- c) an identification authenticating component incorporated into one of said devices and providing a unique identification signal corresponding to the unique identity thereof; and
- d) an identification authorizing component capable of determining if

said unique identity is authorized for synchronization and for correspondingly enabling and disabling synchronization between said portable computer and said host system, wherein decryption of encrypted data from said portable computer device is enabled provided said unique identity is authorized and wherein said decryption is disabled if said unique identity is not authorized.

11. (Currently Amended) A system as recited in Claim 10 wherein said portable computer device comprises is a palmtop computer.

12. (Currently Amended) A system as recited in Claim 10 wherein said portable computer device comprises is a palmtop computer cradle.

13. (Currently Amended) A system as recited in Claim 10 wherein said synchronous communication is further encrypted with a specific key value from said identification authenticating tagging component such that unauthorized applications external to said portable computer system are locked out from deciphering data therefrom.

14. (Currently Amended) A system as recited in Claim 10 wherein said identification authenticating tagging component is a magnetic key and said identification authentication reading component is a magnetic key reader.

15. (Currently Amended) A system as recited in Claim 10 wherein said identification authenticating tagging component is a smart card and said identification authentication reading component comprises is a smart card reader.

16. (Currently Amended) A system as recited in Claim 10 wherein said

identification authorizing component comprises is an application specific integrated circuit.

17. (Currently Amended) A system as recited in Claim 10 wherein said identification authorizing component comprises is a software program.

18. (Currently Amended) A system as recited in Claim 10 wherein said identification authenticating tagging component is in direct electrical connection with said identification authentication reading component via contacts.

19. (Currently Amended) A system as recited in Claim 10 wherein said identification authenticating tagging component is in contact free communication with said identification authentication reading component via an infrared communication mechanism.

20. (Currently Amended) A system as recited in Claim 10 or wherein said identification authenticating tagging component is in contact free communication with said identification authentication reading component via a transmitter/receiver modality and antenna array.

21. (Currently Amended) A system for preventing unauthorized transfer of data between a portable computer system and a system of data storage and communication, comprising:

- a) a portable computer device capable of synchronizing with said system of data storage and communication;
- b) an interface device compatible to receive said portable computer device

and coupled with said system of data storage and communication and capable of facilitating communication between said portable computer device and said system of data storage and communication;

c) an identification authenticating tagging and data encryption keying component incorporated into one of said devices and providing a unique identification signal and an encryption key cipher value corresponding to the unique identity thereof;

d[[.]])) an identification authentication reading component capable of sensing and reading said unique identification signal incorporated into the other of said devices not incorporating said tagging component;

e[[.]])) an identification authorizing component receiving input from said reading component and incorporated into the same one of said devices as said reading component, capable of determining if said unique identity is authorized for synchronization and of correspondingly enabling and disabling synchronization between said portable computer and said system of data storage and communication; and

f[[.]])) an identification authorizing component further capable of enabling deciphering of encrypted communication from said portable computer device if said unique identity is authorized and disabling decryption if said unique identity is unauthorized.

22. (Currently Amended) A system as recited in Claim 20 wherein said identification authorizing component incorporates software for determining if said unique identity is authorized for synchronization, for correspondingly enabling and disabling synchronization, and deciphering encrypted data from said portable computer device.

23. (Currently Amended) A communication system comprising:  
a host computer system comprising a communication port;  
a portable electronic device comprising a communication port and an identity reference; and  
a communication module for coupling between said communication ports of said portable electronic device and said host computer system, said communication interface module comprising:  
an authentication device for authenticating said identity reference; and  
a communication interface circuit coupled to said authentication device and for allowing direct communication between said portable electronic device and said host computer system provided said authentication device indicates a proper authentication of said identity reference and, otherwise, for disallowing communication between said portable electronic device and said host computer system, wherein decryption of encrypted data from said portable computer device is enabled provided said unique identity is authorized and wherein said decryption is disabled if said unique identity is not authorized.

24. (Currently Amended) A communication system as recited described in Claim 23 wherein said communication interface circuit comprises a decryption circuit.

25. (Currently Amended) A communication system as recited described in Claim 23 wherein said communication module contains a slot for receiving said communication port of said electronic device.

26. (Currently Amended) A communication system as recited described in Claim 23 wherein said identity reference is stored on a removable smart card.